Notice of Allowability	Application No.	Applicant(s)	
	09/370,384	ZUCKER, DANIEL F.	
	Examiner	Art Unit	
	Matthew B Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an amendment filed on May 24, 2004*.

2. ☒ The allowed claim(s) is/are *3-6,9-14,17-20,25 and 26; renumbered as 1-16*.

3. ☒ The drawings filed on *24 May 2004* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 24052004
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. David Heid on December 1, 2004.

The application has been amended as follows:

IN THE CLAIMS:

1. (Cancelled)

2. (Cancelled)

3. (Currently Amended) A method for key management, comprising:

generating a set of encrypted bits at a security server:

transmitting said set of encrypted bits from said security server to an application server;

broadcasting said set of encrypted bits from said application server to a plurality of recipients, said set of encrypted bits comprising information for generating a set of encryption/decryption bits;

transmitting said set of encrypted bits from a first recipient to said security server;

authenticating said first recipient at said security server;

transmitting a first set of bits from said security server to said first recipient if said first recipient is authenticated, said first set of bits being a subset of said set of encrypted bits in decrypted form and comprising information for generating a set of encryption bits:

generating said set of encryption bits at said first recipient from said first set of bits;

encrypting a data stream at said first recipient using said set of encryption bits to form a first encrypted data stream; and

broadcasting said first encrypted data stream from said first recipient with said set of encrypted bits to a plurality of receivers;

wherein said set of encrypted bits further comprises information selected from the

group consisting of a policy, a message digest and a ~~data~~ date and time stamp, and further

wherein said policy comprises information selected from the group consisting of security levels of said recipients and classification of said data stream.

4. (Previously Amended) The method of Claim 3, wherein said authenticating comprises:

establishing a private access line ("PAL") between said security server and said first recipient, comprising:

transmitting an identification of said first recipient to said security server;

decrypting said set of encrypted bits at said security server to obtain access information; and

comparing said identification to said access information to establish authentication when said identification matches said access information.

5. (Previously Amended) The method of Claim 3, further comprising:

transmitting said set of encrypted bits from a first receiver to said security server;

authenticating said first receiver at said security server;

transmitting a second set of bits from said security server to said first receiver if said first receiver is authenticated, said second set of bits being a subset of said set of encrypted bits in decrypted form and comprising information for generating a set of decryption bits;

generating at said first receiver said set of decryption bits from said second set of bits; and

decrypting said first encrypted data stream using said set of decryption bits at said first receiver.

6. (Previously Amended) The method of Claim 3, wherein said broadcasting said first encrypted data stream further comprises:

dividing said first encrypted data stream into a plurality of data sections; and

attaching said set of encrypted bits to each of said data sections, each said data section having a corresponding offset value, said offset value is an offset between the starting address of said first encrypted data stream and the starting address of said data section.

7. (Cancelled)

8. (Cancelled)

9. (Previously Amended) The method of Claim 10, further comprising returning a set of bits corresponding to a stored set of encrypted bits from said memory if said set of encrypted bits matches said stored set of encrypted bits.

10. (Previously Amended) A method for key management, comprising:

generating a set of encrypted seal bits at a security server;

transmitting said set of encrypted bits from said security server to an application server;

broadcasting said set of encrypted bits from said application server to a plurality of recipients, said set of encrypted bits comprising information for generating a set of encryption/decryption bits;

transmitting said set of encrypted bits from a first recipient to said security server;

authenticating said first recipient at said security server;

transmitting a first set of bits from said security server to said first recipient if said first recipient is authenticated, said first set of bits being a subset of said set of encrypted bits in decrypted form and comprising information for generating a set of encryption bits;

generating said set of encryption bits at said first recipient from said first set of bits;

encrypting a data stream at said first recipient using said set of encryption bits to form a first encrypted data stream; and

broadcasting said first encrypted data stream from said first recipient with said set of encrypted bits to a plurality of receivers;

wherein said application server comprises a memory for storing said set of encrypted bits and a corresponding set of bits containing said information for generating a set of encryption/decryption bits;

further comprising comparing said set of encrypted bits to a plurality of sets of encrypted bits in said memory;

wherein said set of encrypted bits fails to match any of said stored set of encrypted bits in said memory, further comprising;

transmitting an identification of said first receiver to said security server;

decrypting said set of encrypted bits at said security server to obtain access information; and

comparing said identification of said receiver to said access information to establish authentication set of encrypted bits and when said identification matches said access information.

11. (Previously Presented) The method of Claim 10, further comprising storing said corresponding set of bits containing said information for generating a set of encryption/decryption bits in said memory subsequent to said authentication.

12. (Previously Presented) The method of Claim 3, further comprising deleting a least recently used set of encrypted bits and its corresponding set of bits from said memory when said memory is full.

13. (Previously Amended) The method of Claim 3, further comprising broadcasting said first encrypted data stream in datagram packets, wherein said set of encrypted bits is attached to each of said datagram packets.

14. (Presently amended) A method for key management, comprising:

generating a set of encrypted seal bits at a security servers;

transmitting said set of encrypted bits from said security server to an application server;

broadcasting said set of encrypted bits from said application server to a plurality of recipients, said set of encrypted bits comprising information for generating a set of encryption/decryption bits;

transmitting said set of encrypted bits from a first recipient to said security server;

authenticating said first recipient at said security server;

transmitting a first set of bits from said security server to said first recipient if said first recipient is authenticated, said first set of bits being a subset of said set of encrypted bits in decrypted form and comprising information for generating a set of encryption bits;

generating said set of encryption bits at said first recipient from said first set of bits;

encrypting a data stream at said first recipient using said set of encryption bits to form a first encrypted data stream: and

broadcasting said first encrypted data stream from said first recipient with said set of encrypted bits to a plurality of receivers, further comprising;

appending said set of encrypted bits to said first encrypted data stream; and

transmitting a second encrypted data stream from said first receiver to said first recipient, wherein a second set of encrypted bits is appended to said second encrypted data stream.

15. (Cancelled)

16. (Cancelled)

17. (Previously Amended) The method of claim 18, further comprising returning a permit corresponding to a first previously opened seal from said memory if said seal matches said first previously opened seal.

18. (Previously Amended) A method for opening a seal, wherein said seal comprises a set of encrypted bits comprising information for generating a set of encryption/decryption bits, comprising;

providing a client having memory for storing previously opened seals and their corresponding permits, each of said permits being a subset of a corresponding seal and containing information for generating said set of encryption/decryption bits;

transmitting said seal from a security server to said client; and

comparing said seal to said previously opened seals in said memory, further comprising:

transmitting said seal and identification from said client to said security server if said seal fails to match any of said previously opened seals in said memory;

decrypting said seal at said security server to obtain access information; and

comparing said identification with said access information to obtain authentication if said identification matches said access information.

19. (Previously Presented) The method of Claim 18, further comprising storing said seal and its corresponding permit in said memory if said client is authenticated.

20. (Previously Presented) The method of Claim 18, further comprising deleting a least recently used previously opened seal and its corresponding permit when said memory is full prior to said storing.

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Cancelled)

25. (Previously Amended) A method for key exchange and synchronization over a duplex channels comprising:

transmitting a first encrypted data stream having a first seal appended to the head of said first encrypted data stream from a first party to a second party, said first seal being a first set of encrypted bits comprising information for generating a first setof encryption/decryption bits;

transmitting a second encrypted data stream having a second seal appended to the head of said second data stream from said second party to said first party, said second seal being a second set of encrypted bits comprising information for generating a second set of encryption/decryption bits;

transmitting said first seal from said second party to a security server;

authenticating said second party at said security server;

transmitting a first permit from said security server to said second party if said second party is authenticated, said first permit being a subset of said first seal, in decrypted form, and containing information for encrypting/decrypting said first encrypted data stream;

generating a first set of decryption bits at said second party;

decrypting said first encrypted data stream at said second party using said first set of decryption bits: the method further comprising:

transmitting said second seal from said first party to said security server;

authenticating said first party at said security server; and

transmitting a second permit from said security server to said first party if said first party is authenticated, said second permit being a subset of said second seal, in decrypted form, and containing information for encrypting/decrypting said second encrypted data stream.

26. (Previously Presented) The method of Claim 25, further comprising:

generating a second set of decryption bits at said first party; and

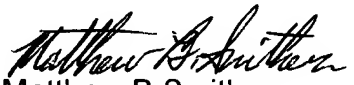
decrypting said second encrypted data stream at said first party using said second set of decryption bits.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew T Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew B Smithers
Primary Examiner
Art Unit 2137